UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/924,391	08/07/2001	Tal Givoly	XACTP001	6261

28875 7590 11/21/2003

SILICON VALLEY INTELLECTUAL PROPERTY GROUP
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
TRAN, PHILIP B	

ART UNIT	PAPER NUMBER
2155	10

DATE MAILED: 11/21/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

PRY

Office Action Summary	Application No.	Applicant(s)	
	09/924,391	GIVOLY, TAL	
	Examiner	Art Unit	
	Philip B Tran	2155	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 September 2003*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

Response to Amendment

1. This office action is in response to the amendment filed on 9/24/2003. Claims 1, 11 and 20-23 have been amended. Therefore, claims 1-23 are presented for further examination.

Response to Arguments

2. Applicants' arguments have been fully considered but they are not persuasive because of the following reasons :

In response to applicant's arguments that cited reference teaches away from the invention of the instant application, the law of anticipation requires that a distinction be made between the invention described or taught and the invention claimed. It does not require that the reference "teach" what the subject patent teaches. Assuming that a reference is properly "prior art," it is only necessary that the claims under consideration "read on" something disclosed in the reference, i.e., all limitations of the claim are found in the reference, or "fully met" by it. ***Colman v. Kimberly-Clark Corp.*****, 218 USPO 789.**

Conklin teaches a method for processing network accounting information, comprising receiving accounting information over a packet-switched network, monitoring at least one aspect of the received accounting information, and discarding at least a portion of the accounting information that occurs during a surge in network traffic, based on the monitored aspect. For example, network traffic measurement and monitoring for reporting information about captured packets reflecting activities of intrusions and detecting intrusions into the network and into computers connected to the network for

denial of services [see Abstract and Figs. 6-9 and Col. 1, Line 10 - Col. 2, Line 4 and Col. 5, Line 22 – Col. 6, Line 43].

The examiner notes that applicant's arguments are not directed to the important functions carried out as indicated in the limitations of independent claims. Instead, applicant misinterprets the terminologies when comparing the limitations of independent claims with the applicant's quoted paragraph from Conklin. Essentially, applicant argues merely based on the wording of "discarded". With respect to Conklin, Conklin teaches capabilities of monitoring network intrusions in real-time [see Abstract] and logging monitoring events for appropriate response activities against intrusions such as restoring lost data, removing unauthorized programs, or disconnecting the system from the network temporarily [see Col. 6, Lines 40-43] and therefor discarding at least a portion of the accounting information that occurs during a surge in network traffic, based on the monitored aspect as claimed by applicant.

Therefore, the examiner asserts that Conklin teaches or suggests the subject matter broadly recited in independent claims 1, 11 and 20-22. Claim 23 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Conklin in view of Savoldi and further in view of Trcka. Claims 2-10 and 12-19 are also rejected at least by virtue of their dependency on independent claims. Accordingly, claims 1-23 are respectfully rejected as shown below.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless --

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-4, 6-8, 10-17, and 20-22 are rejected under 35 U.S.C. § 102(e) as being anticipated by Conklin et al (Hereafter, Conklin), U.S. Pat. No. 5,991,881.

Regarding claim 1, Conklin clearly teaches a method for processing network accounting information, comprising receiving accounting information over a packet-switched network, monitoring at least one aspect of the received accounting information, and discarding at least a portion of the accounting information that occurs during a surge in network traffic, based on the monitored aspect (i.e., network traffic measurement and monitoring for reporting information about captured packets reflecting activities of intrusions and detecting intrusions into the network and into computers connected to the network for denial of services) [see Abstract and Figs. 6-9 and Col. 1, Line 10 - Col. 2, Line 4 and Col. 5, Line 22 – Col. 6, Line 43].

Regarding claim 2, Conklin further teaches the method as recited in claim 1, wherein the accounting information is discarded for providing a defense against network attacks (i.e., against network intruder) [see Abstract and Col. 6, Line 34-43].

Regarding claim 3, Conklin further teaches the method as recited in claim 1, wherein the accounting information is discarded for dealing with heavy network traffic (i.e., monitoring and analyzing the traffic communication) [see Fig. 6].

Regarding claim 4, Conklin further teaches the method as recited in claim 3, and further comprising generating a summary of the accounting information (i.e., reported of collected information and stored information in the database) [see Col. 4, Line 52 - Col. 5, Line 45].

Regarding claim 6, Conklin further teaches the method as recited in claim 1, wherein monitoring the at least one aspect of the received accounting information includes detecting a scan of a plurality of Internet Protocol (IP) addresses (i.e., detecting IP address) [see Col. 5, Lines 26-45 and Col. 6, Lines 44-60].

Regarding claims 7-8, Conklin further teaches the method as recited in claim 1, wherein monitoring the at least one aspect of the received accounting information includes monitoring a rate of receipt of the accounting information and whether the rate of receipt of the accounting information exceeds a predetermined amount (i.e., monitoring and collecting network data such as traffic over time) [see Figs. 6-8 and Col. 4, Lines 30-67].

Regarding claim 10, Conklin further teaches the method as recited in claim 1, wherein the network includes the Internet (i.e., using TCP/IP suggests the network attached to the Internet) [see Col. 3, Lines 15-21].

Claim 11 is rejected under the same rationale set forth above to claim 1.

Claims 12-14 are rejected under the same rationale set forth above to claims 2-4, respectively.

Claims 15-17 are rejected under the same rationale set forth above to claims 6-8, respectively.

Claims 20-22 are rejected under the same rationale set forth above to claim 1.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 5 and 18 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Conklin et al (Hereafter, Conklin), U.S. Pat. No. 5,991,881 in view of Savoldi et al (Hereafter, Savoldi), U.S. Pat. No. 5,727,146.

Regarding claim 5, Conklin does not explicitly teach the method as recited in claim 1, wherein monitoring the at least one aspect of the received accounting information includes detecting a scan of a plurality of ports. However, portscan detection is well-known in the art as disclosed by Savoldi [see Abstract and Col. 1, Line 61 - Col. 2, Line 30 and Col. 2, Line 53 - Col. 3, Line 3]. It would have been obvious to one of

ordinary skill in the art at the time of the invention was made to scan the ports in order to track down ongoing attacks and identifying potential intrusions on the network and system connected to the network.

Claim 18 is rejected under the same rationale set forth above to claim 5.

7. Claims 9 and 19 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Conklin et al (Hereafter, Conklin), U.S. Pat. No. 5,991,881 in view of Trcka et al (Hereafter, Trcka), U.S. Pat. No. 6,453,345.

Regarding claim 9, Conklin does not explicitly teach the method as recited in claim 1, wherein monitoring the at least one aspect of the received accounting information includes monitoring a load on a system receiving the accounting information. However, monitoring and collecting statistic information such as traffic load is well-known in the art as disclosed by Trcka [see Col. 21, Lines 24-28]. It would have been obvious to one of ordinary skill in the art at the time of the invention was made to monitor a load on the system in order to avoid traffic congestion and overload problems.

Claim 19 is rejected under the same rationale set forth above to claim 9.

8. Claim 23 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Conklin et al (Hereafter, Conklin), U.S. Pat. No. 5,991,881 in view of Savoldi et al (Hereafter, Savoldi), U.S. Pat. No. 5,727,146 and further in view of Trcka et al (Hereafter, Trcka), U.S. Pat. No. 6,453,345.

Regarding claim 23, Conklin teaches a method for processing network accounting information, comprising receiving accounting information over a packet-switched network, monitoring at least one aspect of the received accounting information, and discarding at least a portion of the accounting information based on the monitored aspect (i.e., network traffic measurement and monitoring for reporting information about captured packets and detecting intrusion into the network and into computers connected to the network for denial of service) [see Abstract and Figs. 6-9 and Col. 1, Line 10 - Col. 2, Line 4]. Conklin further teaches generating a summary of the accounting information (i.e., reported of collected information and stored information in the database) [see Col. 4, Line 52 - Col. 5, Line 45], detecting a scan of a plurality of Internet Protocol (IP) addresses (i.e., detecting IP address) [see Col. 5, Lines 26-45 and Col. 6, Lines 44-60], and monitoring a rate of receipt of the accounting information and whether the rate of receipt of the accounting information exceeds a predetermined amount (i.e., monitoring and collecting network data such as traffic over time) [see Figs. 6-8 and Col. 4, Lines 30-67]. Conklin does not explicitly teach detecting a scan of a plurality of ports. However, portscan detection is well-known in the art as disclosed by Savoldi [see Abstract and Col. 1, Line 61 - Col. 2, Line 30 and Col. 2, Line 53 - Col. 3, Line 3]. It would have been obvious to one of ordinary skill in the art at the time of the invention was made to scan the ports in order to track down ongoing attacks and identifying potential intrusions on the network and system connected to the network. In addition, Conklin does not explicitly teach monitoring a load on a system receiving the accounting information. However, monitoring and collecting statistic information such as traffic load is well-known in the art as disclosed by Trcka [see Col. 21, Lines 24-28]. It

would have been obvious to one of ordinary skill in the art at the time of the invention was made to monitor a load on the system in order to avoid traffic congestion and overload problems.

Conclusion

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CAR 1.136(a).

A SHORTENED STATUTORY PERIOD FOR REPLY TO THIS FINAL ACTION IS SET TO EXPIRE THREE MONTHS FROM THE MAILING DATE OF THIS ACTION. IN THE EVENT A FIRST REPLY IS FILED WITHIN TWO MONTHS OF THE MAILING DATE OF THIS FINAL ACTION AND THE ADVISORY ACTION IS NOT MAILED UNTIL AFTER THE END OF THE THREE-MONTH SHORTENED STATUTORY PERIOD, THEN THE SHORTENED STATUTORY PERIOD WILL EXPIRE ON THE DATE THE ADVISORY ACTION IS MAILED, AND ANY EXTENSION FEE PURSUANT TO 37 CAR 1.136(A) WILL BE CALCULATED FROM THE MAILING DATE OF THE ADVISORY ACTION. IN NO EVENT, HOWEVER, WILL THE STATUTORY PERIOD FOR REPLY EXPIRE LATER THAN SIX MONTHS FROM THE MAILING DATE OF THIS FINAL ACTION.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Philip Tran whose telephone number is (703) 308-8767. The Group fax phone number is (703) 872-9306.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hosain T. Alam, can be reached on (703) 308-6662.

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (703) 305-3900.

PBT
Philip Tran
Art Unit 2155
Nov 19, 2003

FRANTZ B. JEAN
PRIMARY EXAMINER